Sherry S. Hamilton, SBN 262093
shamilton@mortensontaggart.com
Kevin A. Adams, SBN 239171
kadams@mortensontaggart.com
MORTENSON TAGGART ADAMS LLP
300 Spectrum Center Dr., Suite 1200
Irvine, CA 92618
Telephone: (949) 774-2224
Facsimile: (949) 774-2545

Attorney for Plaintiff
TODD GLASS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TODD GLASS,

Plaintiff,

vs.

DOCUSIGN, INC.; and DOES 1 through 10, inclusive,

Defendant.

CASE NO.

COMPLAINT FOR:

(1) VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (18 U.S.C. § 2511(1)(a));

(2) VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (18 U.S.C. § 2511(1)(c) & (d)); AND

(3) VIOLATION OF THE STORED COMMUNICATIONS ACT (18 U.S.C. § 2701)

Plaintiff Todd Glass brings this Complaint against Defendant DocuSign, Inc., and states the following:

INTRODUCTION

1. DocuSign, Inc., is a company that provides, among other things, secure electronic signature products and services to its customers and users. DocuSign is widely used to authenticate the electronic signatures of individuals that are placed on legal documents, such as contracts, deeds, and court filings.

2. Although DocuSign purports to be a secure, encrypted service, its electronic signature system is vulnerable to outside malware and hackers. Specifically, DocuSign can be used to facilitate access to private communications and documents stored on the computers of DocuSign customers and users. As further detailed in this Complaint, Defendants have violated federal law by allowing third-party hackers to hijack the DocuSign system to access Plaintiff's private communications and documents.

3. Plaintiff has asked Defendant for assistance to determine the methodology used by the hackers to breach the DocuSign system, and also to preserve documents, records, and data to assist in the investigation of the breach of Plaintiff's computer, documents, and communications. Defendant has refused Plaintiff's request and has responded that its policies only require the company to maintain documents signed through the DocuSign system for fourteen days. The breach to Plaintiff's computer, documents, and communications occurred on February 13, 2023, and the fourteen-day document retention period expires on February 27, 2023. Given that destruction of evidence by DocuSign is apparently imminent, Plaintiff has been forced to file this Complaint to ensure that the spoliage of evidence by Defendant does not occur.

4. In facilitating the breach of Plaintiff's computer, documents, and communications, Defendant intentionally, wantonly, and maliciously violated the Electronic Communications Privacy Act (18 U.S.C. § 2511) and the Stored

Communications Act (18 U.S.C. § 2701).

PARTIES

5. Plaintiff Todd Glass is an individual who resides in Fairfax County, Virginia. He is a person that uses Defendant's electronic signature authentication system.

6. Defendant DocuSign, Inc., is a Delaware corporation with its principal place of business located in San Francisco, California. Defendant provides electronic signature authentication products and services throughout the nation.

JURISDICTION AND VENUE

7. This Court has original jurisdiction over the Stored Communications Act claims within this Complaint pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2707.

8. This Court has original jurisdiction over the Electronic Communications Privacy Act claims within this Complaint pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2520.

9. This Court has personal jurisdiction over Defendants because it has its principal place of business and conducts business in this judicial district.

10. Venue is proper pursuant to 28 U.S.C. §§ 1391(b)(1) and (2) because Defendant's headquarters are located in this judicial district and, alternatively, because a substantial part of the events or occurrences giving rise to Plaintiff's claims occurred in this judicial district.

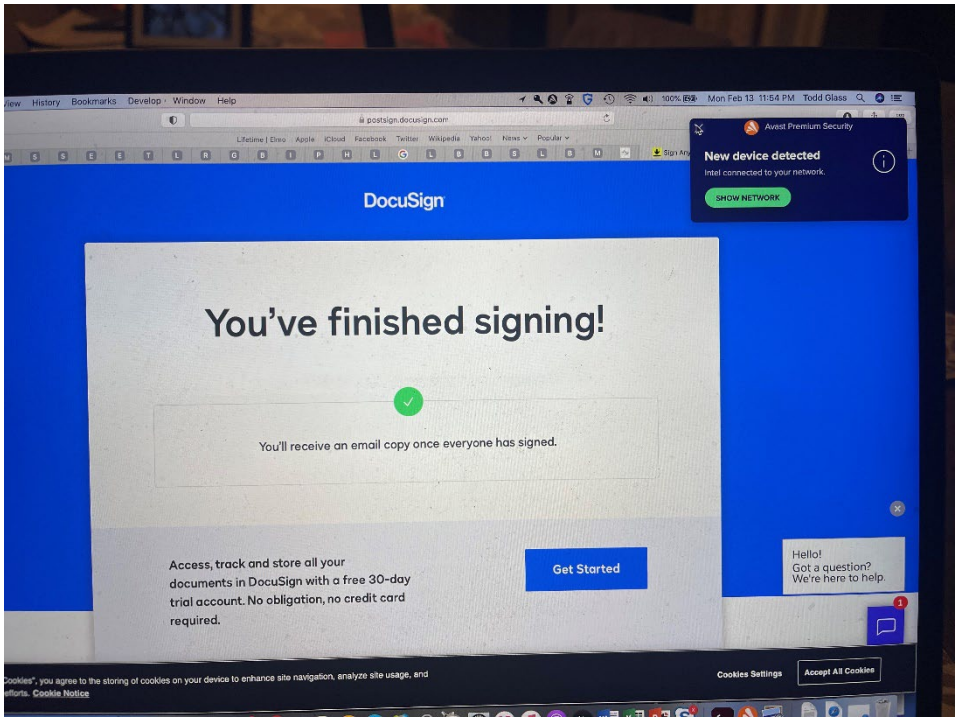
FACTS

11. On February 13, 2023, Plaintiff's counsel in an unrelated case (who is not counsel of record here) requested that Plaintiff electronically sign documents for a court submission via the DocuSign system.

///

///

12. Pursuant to that request, Plaintiff accessed the DocuSign system and executed his electronic signature on the documents as requested via the DocuSign website. When Plaintiff clicked on the "Finish" button to complete his signature, his security software alerted him that a new device had connected to his computer. An image of the alert is shown below.



13. The DocuSign system assigned unique document identifiers to the documents Plaintiff signed. The DocuSign system assigned Security Code 3CC2C8E37D0E49E0970E1FAF66FE7F047 to the document to be reviewed by Plaintiff, and assigned DocuSign Envelope ID = 6B3DC5D3-4517-4877-A1E0-364F4DBE50D2 to each page of the document. Images of the security code and envelope ID are below.

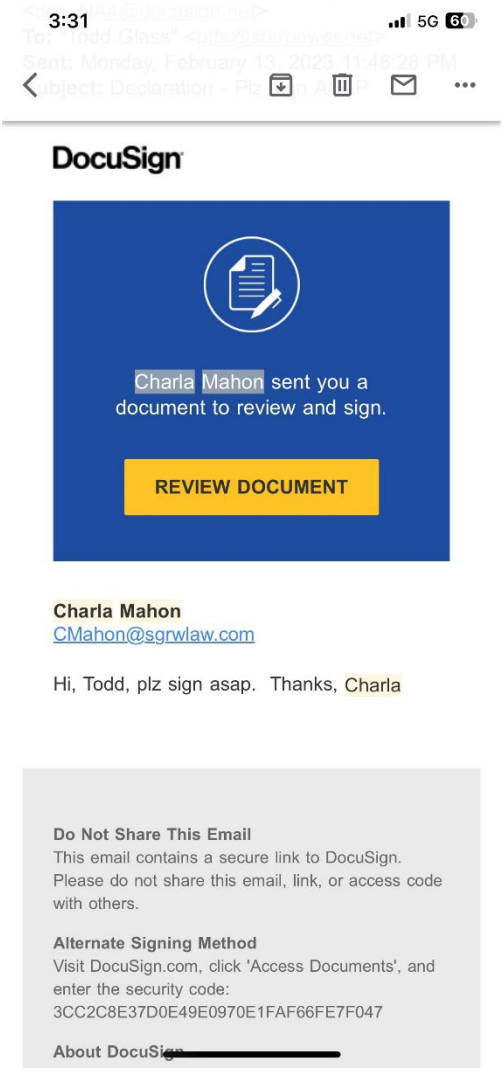
///

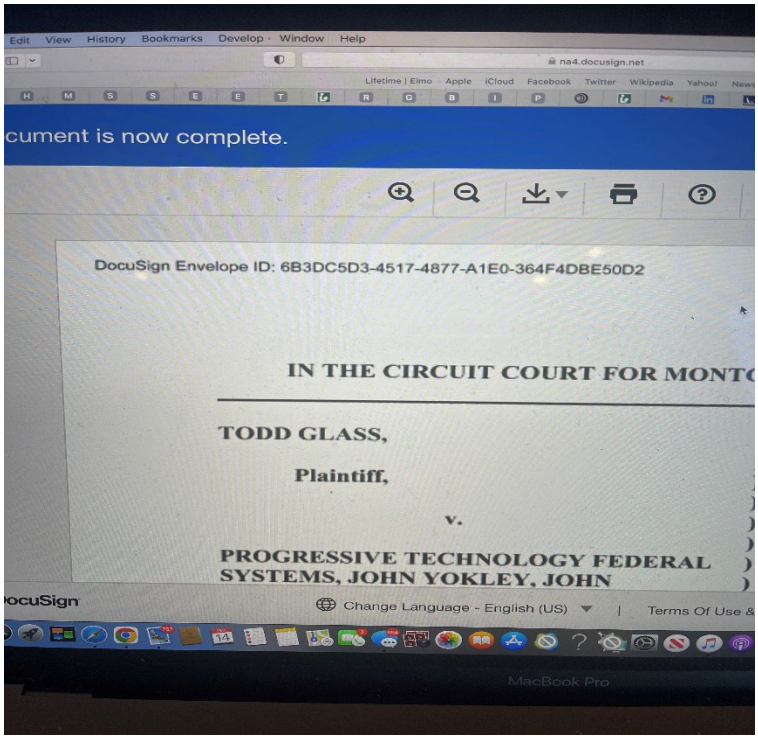
///

///

///

///


3:31
5G
DocuSign
Charla Mahon sent you a document to review and sign.
REVIEW DOCUMENT
Charla Mahon
CMahon@sgrwlaw.com
Hi, Todd, plz sign asap. Thanks, Charla
Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.
Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code:
3CC2C8E37D0E49E0970E1FAF66FE7F047
About DocuSign


cument is now complete.
DocuSign Envelope ID: 6B3DC5D3-4517-4877-A1E0-364F4DBE50D2
IN THE CIRCUIT COURT FOR MONT
TODD GLASS,
Plaintiff,
v.
PROGRESSIVE TECHNOLOGY FEDERAL SYSTEMS, JOHN YOKLEY, JOHN
Change Language - English (US)
Terms Of Use &
MacBook Pro

14. Upon seeing the alert from his security software that a new device had attached to his computer, Plaintiff immediately became concerned that the security of his computer, communications, and documents had been compromised. Plaintiff contacted his IT security consultant who conducted an investigation to confirm that his systems had been breached. This breach potentially included access to Plaintiff's computer, communications, and documents. However, further information would be required from DocuSign in order to ascertain the nature, source, and full extent of the breach.

15. Plaintiff contacted DocuSign representatives to attempt to secure the company's cooperation for the breach investigation. During the calls, Plaintiff learned that the DocuSign system was apparently vulnerable to hacking, and that the company had not taken appropriate steps to secure the system to prevent threat actors from using the DocuSign system to deliver malware or utilize hacking techniques to access a victim's computer systems.

16. Rather than reporting to Defendant's cyber security team that Plaintiff's system had been breached using the DocuSign system, Defendant's representatives merely directed Plaintiff to the company's online policies without providing any further assistance. Those policies stated that DocuSign would only retain documents for fourteen days before they would be deleted.

CLAIMS FOR RELIEF

COUNT ONE: VIOLATION OF 18 U.S.C. § 2511(1)(a) – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

17. Plaintiff incorporates and re-alleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

18. At all relevant times herein, subject to specific exceptions (not applicable here), 18 U.S.C. § 2511(1)(a) prohibited the intentional interception of any electronic communications between two parties without the consent of one or both parties to that communication.

19. By engaging in the conduct described above, Defendant intentionally and contemporaneously intercepted Plaintiff's electronic communications, without their consent, thereby violating 18 U.S.C. § 2511(1)(a).

20. Defendant's actions were unlawful, willful, wanton, and malicious, and were intended for the purpose of harming Plaintiff.

21. Pursuant to 18 U.S.C. § 2520, Plaintiff are entitled to relief for Defendant's violations of 18 U.S.C. § 2511(1)(a).

22. By reason of the foregoing, as a result of Defendant's conduct described herein, Plaintiff are entitled to recover the maximum statutory damages, punitive damages, and attorney's fees and costs available under 18 U.S.C. § 2520.

COUNT TWO: VIOLATION OF 18 U.S.C. §§ 2511(1)(c) & (d) – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

23. Plaintiff incorporates and re-alleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

24. At all relevant times herein, 18 U.S.C. § 2511(1)(c) prohibited the intentional disclosure, or endeavor to disclose, to any other person the contents of any electronic communication, knowing or having reason to know that the information was obtained through the interception of an electronic communication.

25. At all relevant times herein, 18 U.S.C. § 2511(1)(d) prohibited the intentional use, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

26. After illegally intercepting private and confidential emails intended for Plaintiff, Defendant intentionally disclosed and used Plaintiff's electronic communications.

///

27. Defendant knew, should have known, or had reason to know that the electronic communications from Plaintiff's email accounts were obtained through the interception of electronic communications.

28. By engaging in the foregoing conduct, Defendant violated 18 U.S.C. §§ 2511(1)(c) & (d).

29. At all relevant times, Defendants did not have authorization to use or disclose Plaintiff's electronic communications.

30. Defendant's actions were unlawful, willful, wanton, and malicious, and were intended for the purpose of harming Plaintiff.

31. Pursuant to 18 U.S.C. § 2520, Plaintiff are entitled to relief for the Defendant's violations of 18 U.S.C. § 2511(1)(c) & (d).

32. By reason of the foregoing, as a result of Defendant's conduct described herein, Plaintiff are entitled to recover the maximum statutory damages, punitive damages, and attorney's fees and costs available under 18 U.S.C. § 2520.

COUNT THREE: VIOLATION OF 18 U.S.C. § 2701 – STORED COMMUNICATIONS ACT

33. Plaintiff incorporates and re-alleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

34. At all relevant times, the Stored Communications Act ("SCA") (18 U.S.C. § 2701 et seq.) was in full force and effect and governed the accessing of facilities through which electronic communication service is provided.

35. The SCA broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . ." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(12).

36. Pursuant to the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic

transmission thereof." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their recipient.

37. Congress enacted the SCA to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99-541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

38. As such, the SCA mandates that it is unlawful for a person to intentionally access without authorization a facility through which an electronic communication service is provided, or intentionally exceed an authorization to access that facility. 18 U.S.C. § 2701(a).

39. On February 13, 2023, Defendant violated 18 U.S.C. § 2701(a) by intentionally and without Plaintiff's authorization, accessing electronic communications intended for Plaintiff while said electronic communications were in electronic storage systems.

40. Pursuant to 18 U.S.C. § 2707, Plaintiff are entitled to relief for Defendant Estrada's violations of 18 U.S.C. § 2701(a).

41. By reason of the foregoing, as result of Defendant's conduct described herein, Plaintiff seek recovery of the maximum statutory damages, punitive damages, and attorney's fees and costs available under 18 U.S.C. § 2707.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff request a trial by jury and that judgment be entered against Defendants as follows:

1. Statutory damages as authorized under the Electronic Communications Privacy Act and/or the Stored Communications Act pursuant to 18 U.S.C. § 2707(c) and 18 U.S.C. § 2520(c);

///

///

2. Punitive damages as authorized under the Electronic Communications Privacy Act and/or the Stored Communications Act pursuant to 18 U.S.C. § 2707(c) and 18 U.S.C. § 2520(b);

3. Attorney's fees and costs pursuant to 18 U.S.C. § 2520(b) and 18 U.S.C. § 2707(b); and

4. Such further and additional relief as this Court may find to be fair and equitable.

DATED: February 24, 2023

MORTENSON TAGGART ADAMS LLP

By: 

Kevin A. Adams
Sherry S. Hamilton
Attorney for Plaintiff
TODD GLASS